Indiana Office of Technology (IOT)
Information Technology Policy (ITP) 05-1

Technology Profile: Security / Privacy

Specific Area: Information Technology Security, Incident Response

Purpose: To establish requirements for reporting cyber security incidents

Policy: All *state entities* must report cyber security incidents to the Indiana Office of Technology (IOT) as described in the attached Cyber Security Incident Reporting Procedure. Reporting incidents to a central group promotes collaboration and information sharing with other sites that may be experiencing the same problems. Some of the benefits this provides include the following:

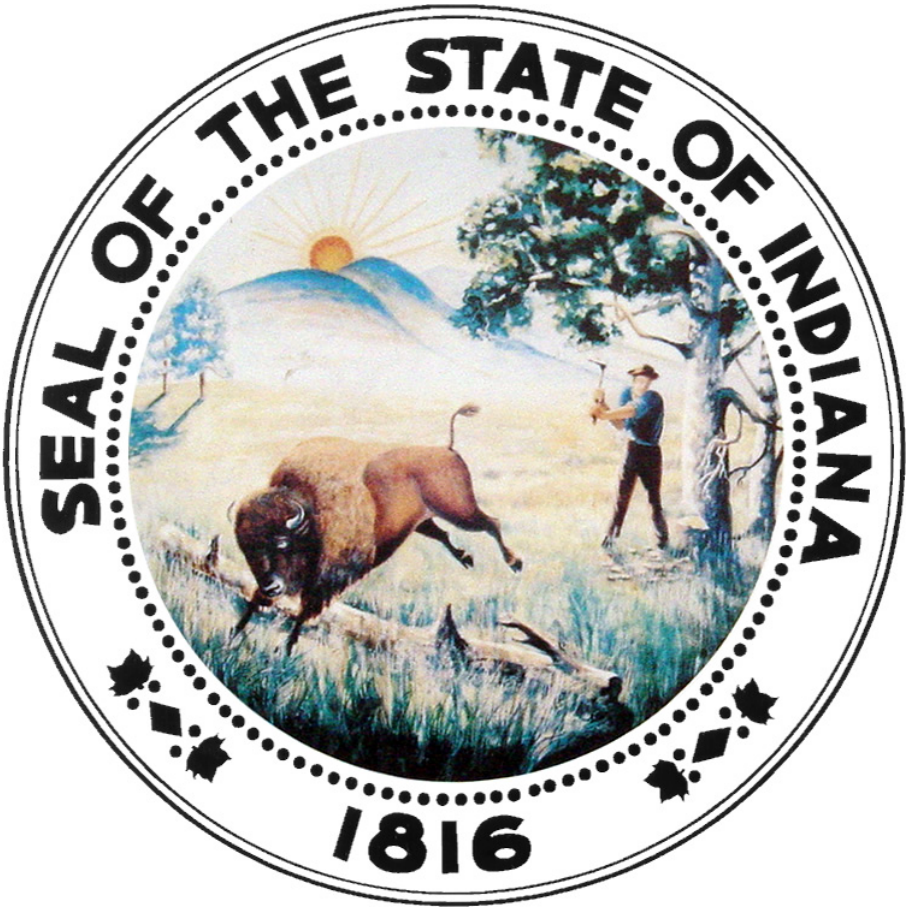
- The ability to coordinate activities among *state entities* experiencing similar incidents to help identify and resolve the problem more quickly than if done separately.
- The ability to coordinate similar *state entities* that may be pursuing legal actions against the intruder.
- The ability to warn and share preventative information to help other *state entities* protect themselves from similar attacks.
- The ability to collect statewide information on the types of vulnerabilities that are being exploited, frequency of attacks and cost of recovering from an attack.

Scope: All state of Indiana governmental bodies connected to the state's back-bone to include all branches of government (executive, administrative, legislative and judicial)

Statutory Authority: IC 4-13.1

References: Cyber Security Incident Reporting Policy

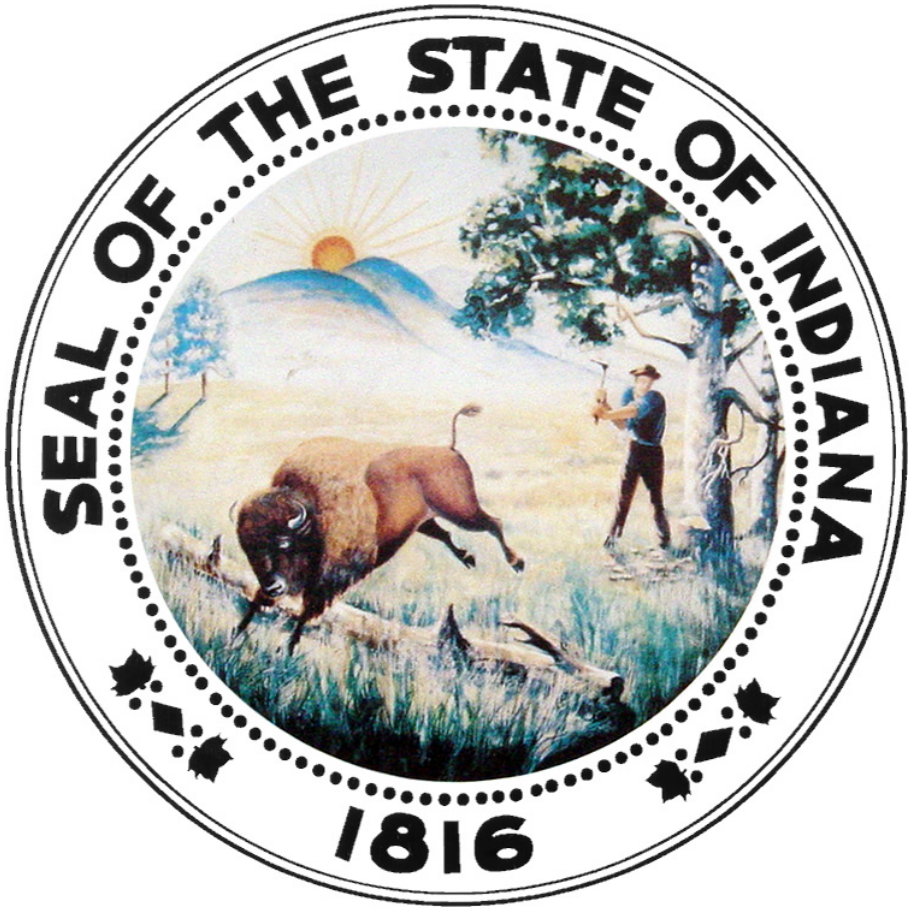
Effective Date: July 1, 2005 (re-issued)



Cyber Security Policy ITP 05-01

Incident Reporting Policy

Issue Date:
Publication Date:



CYBER SECURITY POLICY

Reference:	**ITP 05-01**
Technology Category:	**Security and Privacy**
Policy Title:	**Cyber Incident Reporting**
Replaces & Supersedes:	**Not Applicable**
Authority:	**IC 4-23-16 4.2a**

ITOC is responsible for monitoring agency information technology activities, developing and maintaining policies, procedures, and guidelines for the effective use of information technology, and conducting periodic management reviews of information technology activities within state agencies, regardless of the branch of government.

Issued By:	Information Technology Oversight Commission
Issue Date:	
Publication Date:	
Policy Effective Date:	
Review Date:	**Once per year on adoption date**

TABLE OF CONTENTS

PURPOSE

The purpose of this policy is to direct all *state entities* to report cyber security incidents to Information Technology Oversight Commission (ITOC). Reporting incidents to a central group promotes collaboration and information sharing with other sites that may be experiencing the same problems. Some of the benefits this provides include the following:

- The ability to coordinate activities among *state entities* experiencing similar incidents to help identify and resolve the problem more quickly than if done separately.
- The ability to coordinate similar *state entities* that may be pursuing legal actions against the intruder.
- The ability to warn and share preventative information to help other *state entities* protect themselves from similar attacks.
- The ability to collect statewide information on the types of vulnerabilities that are being exploited, frequency of attacks and cost of recovering from an attack.

POLICY

Part 1. What is a Cyber Security Incident?

A cyber security incident is considered to be any adverse event that threatens the confidentiality, integrity or accessibility of *state entity* information resources. These events include but are not limited to the following malicious activities:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data.
- Unwanted disruption or denial of service.
- Unauthorized use of a system for the transmission, processing or storage of data.
- Changes to system hardware, firmware or software characteristics without the *state entity's* knowledge, instruction or consent.
- Attempts to cause failures in critical infrastructure services, loss of critical supervisory and data acquisition systems.
- Attempts to cause failures that may result in loss of life or have a significant impact on the health or economic security of the state.

Part 2. What Types of Cyber Incidents Should be Reported?

The following types of incidents should be reported to ITOC:

Unauthorized Access

- Report successful, unauthorized access to *state entity* systems (e.g., web site defacements, unauthorized root or administrator access).
- Report unsuccessful attempts only if they are considered to be persistent (e.g., someone from the same source keeps locking out accounts trying to brute force passwords, an automated script keeps probing a *state entity's* web server causing response problems).

- Report suspected unauthorized access, even if unproven, if your agency believes the incident may impact other agencies.

Malicious Code

- Report instances of *viruses*, *Trojan horses*, worms or other malicious code that have had widespread impact or adversely affected one or more mission critical servers at your site.
- Report malicious code blocked by email proxies or other anti-virus software only if it seems to be persistent and beyond current Internet norms.

Denial of Service (*DoS*)

- Report all denial of service attacks that adversely affect or degrade access to critical services.
- Report all other attempted denial of service attacks particularly if they are persistent or significant (e.g., attempted *DoS* attacks aimed specifically at your *DNS* servers or routers would be significant).

Reconnaissance Scans and Probes

- Scans and probes that precede or are related to the incidents listed above should be reported as part of that incident.
- Any other scans and probes should be reported only if they are persistent or significant (e.g. stealthy scans that attempt to avoid detection may be significant versus "*script kiddie*" scans.)

Part 3. Who Should Report Cyber Incidents?

The *state entity's ISO* and his/her designee are responsible for submitting incident reports to ITOC. Reports from any other sources will be validated by ITOC with the affected *state entity ISO* before action is taken.

Part 4. How and When Should Cyber Incidents be Reported?

Urgent Incidents

Urgent incidents should be reported (see Part 5 for information to be reported) to ITOC by calling (317) 232-0184. Reports of these incidents are to be made as close to the time of discovery as is possible.

Examples of urgent incidents include:

- Unauthorized root or administrator access to critical servers, routers, firewalls, etc.
- Wide spread damaging *virus* or worm infection.
- Major outages due to denial of service attacks.
- Mission critical application failures.
- Attacks on mission critical infrastructure services.

Non-Urgent Incidents

Non-urgent incidents should be reported to ITOC by the first business day following detection using one of the following options:

- Call Don Wray, ITOC at (317) 232-0184 and indicate you are reporting a security incident, or
- Fax the report to "Don Wray, ITOC" at (317) 232-0748
- If Don Wray is not available contact Ron Baker, DoIT at (317) 232- 7235

Examples of non-urgent incidents include:

- Major reconnaissance scans and probes.
- Attempted but unsuccessful denial of service attacks.
- Degradation of service attacks.

Part 5. What Information Should be Reported?

Incident reports should contain as much of the following information (see the attached "Incident Notification Report") as is available at that particular time. Additional information such as resource costs in handling the incident may not be known initially but are included here as a reminder that the information should be tracked and reported in a follow up report.

Contact information

- Name
- Organization Name
- Email address
- Phone number(s)

Description of incident

- Date & time incident was detected
- Date & time incident actually occurred (if different from above)
- Type of incident (e.g., web defacement, *virus*/worm
- Method of intrusion (e.g., vulnerability exploited)
- Level of unauthorized access (e.g., root, administrator, user
- Log extracts if appropriate
- Any other relevant information

Affected System(s)

- *IP address* and *hostname*
- Purpose of the system (e.g., *DNS* server, router, e-mail server, XZY application server
- Operating system and software versions and patch levels
- The type of protection that is in place (e.g., firewall, IDS or anti-virus make, model and version)

Attack Source(s)

- *IP address* and *hostname*
- Internal or external source

Damage assessment (estimated)

- Impact of attack on business
- Staff time to detect, handle and recover from the incident
- Costs due to information loss, downtime, etc.

Part 6. Confidentiality of Information

Information regarding specific security measures or security-related incidents will not be publicly disclosed by ITOC. However, to fulfill the intent of this policy ITOC may share information about incidents with other *state entities* after receiving the consent of the affected *state entity's ISO*. This will occur in all cases possible exceptions could be for the following:

- The information pertains to an act of terrorism. In this case the information will be reported to the Director of Counter Terrorism and Security Council,
- Where mandated by law, or
- Where extraordinary circumstances prevent obtaining prior consent from the *ISO*. In these cases ITOC will ensure that the *state entity ISO* is notified as soon as possible after-the-fact.

In the case where the ISO is not permitted, for reasons of security or request from an investigating authority, to complete the attached form, contact Don Wray, ITOC at (317) 232-0184 to set-up a meeting to discuss incident.

Part 7. Document Change Management

A. Requests for changes to this policy should be presented by the *state entity Chief Information Security Officer (CISO)* to the Security and Privacy Technology Architecture Committee. If the state information security officer for the ITOC agrees to the change, he or she will formally draft the change and have it reviewed and approved through normal policy approval process. Each agency *CISO* will be responsible for communicating the approved changes to their organization.

B. This policy and supporting policies and standards will be reviewed minimally on an annual basis.

DEFINITIONS

DNS	The Domain Name System (DNS) provides a translation from names (see *Hostname*) people use to the numbers (see *IP Address*) that computers use.
DoS	A Denial of Service (DoS) attack renders computer applications unavailable for legitimate use by flooding it with more information that the host network or computer system can handle.
Hostname	The name assigned to a computer that is more easily understood by people. Hostnames are normally maintained by the *DNS* (see DNS.)
IP Address	A numeric address required by computers to exchange information.
Information Security Officer (ISO)	The person who has the overall responsibility, for the agency, to ensure the implementation, enhancement, monitoring and enforcement of security policies and standards as defined in the Enterprise Information Technology Security Policy.
Script Kiddie	A teenager that uses scripts written by others to carry out malicious hacking, instead of relying on personal skills or original programs.
State Entity	Any governmental body within the state of Indiana connected to the state's back bone to include all branches of government.
Trojan Horse	A malicious computer application that is hidden in a more useful application. For example a person may download a game from the Internet that also sends personal information back to a malicious Internet site.
Virus	A malicious computer application that is designed to spread itself to other computers. Viruses attach themselves to certain types of computer files and spread when people share those files. A worm is a special type of virus that can spread automatically via e-mail.

CONTACT INFORMATION

Questions concerning this policy may be directed to the *Information Technology Oversight Commission (ITOC) (317)232-0184*.

INCIDENT NOTIFICATION REPORT

Date & Time Reported to ITOC:	
Agency:	
Reported by: ▪ **Name** ▪ **Phone** ▪ **E-mail**	
Nature of Incident: □ **Denial of Service** □ **Malicious Code** □ **Reconnaissance Scans and Probes** □ **Unauthorized Access** □ **Other (describe)**	
Location of Affected Systems: ▪ **Address** ▪ **Building/Room**	
Details: (virus name, events, etc)	
Date & Time Occurred:	
Date & Time Detected:	
How was the Incident detected?	
Describe overall business impact of incident:	
Compromised System Details	
System(s) affected ▪ **Host/node name** ▪ **Network address**	
Hardware involved ▪ **Manufacturer** ▪ **Model**	
O/S ▪ **Version** ▪ **Patch level**	
Compromised account name(s) ▪ **Version** ▪ **Patch level**	
Compromised software	
Source of attack	

Describe What Actions have been taken so far	
Was system removed from network?	
Audit logs recovered and examined? **Which?**	
Forensic backups made? **Original media secured?**	
Describe initial containment measures (firewall, ACL, etc)	
Who has been notified? (e.g. ISP? State Police?) **When notified** ▪ **Date and time**	
Technical contact (System/network administrators)	
Additional Information:	